UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/787,227	02/27/2004	Bach H. Le	049051-0221	4842

31824   7590   10/13/2009
MCDERMOTT WILL & EMERY LLP
18191 VON KARMAN AVE.
SUITE 500
IRVINE, CA 92612-7108

EXAMINER
BELANI, KISHIN G

ART UNIT	PAPER NUMBER
2443	

MAIL DATE	DELIVERY MODE
10/13/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 August 2009*.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *66-68 and 70-87* is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *66-68 and 70-87* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

This action is in response to Applicant's RCE filed on 08-04-2009. **Independent Claims 66, 84, 85 and dependent claims 70, 71, and 82** have been amended. **New dependent claims 86-87 have been added**. The applicants' amendments to claims are shown in ***bold and italics***, and the examiner's response to the amendments is shown in **bold** in this office action. **Claims 66-68 and 70-87** are now pending in the present application.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/04/2009 has been entered.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 87 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention. Claim 87 recites "detection of the user without manual input

from the user", then continues with the text "performed by software configured to use

artificial intelligence to examine input or writing style of another user". It is not clear how

such conflicting claim features will be implemented (without user input followed by input

or writing style of user). Also, the reason for the use of "another user" in the claim text

is unclear. Is the original user not required to provide handwriting sample after leaving

the terminal unattended for a certain period of time?

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth
> in section 102 of this title, if the differences between the subject matter sought to be patented and the prior
> art are such that the subject matter as a whole would have been obvious at the time the invention was
> made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall
> not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating
     obviousness
     or nonobviousness.

This application currently names joint inventors. In considering patentability of

the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

Claims 66, 70, 80, 82, 84 and 85 are rejected under 35 U.S.C. 103(a) as being

unpatentable over **Walker et al. (U.S. Patent Publication # 6,244,957 B1)** in view of

Shaffer et al. (U.S. Patent Publication # 6,145,083).

Consider **claim 66**, Walker et al. show and disclose a computing device for

communicating with a remotely located computing device (Fig. 1 that shows a slot

machine 2 (a computing device) that communicates via slot network 3 with a slot

network server 4 (a remotely located computing device); column 3, line 60 through

column 4, line 18 describe the system shown in Fig. 1; Fig. 2 and column 4, lines 19-29

describe the details of the slot machine 2; Fig. 3 and column 5, lines 21-28 disclose the

details of the slot network server 4), the computing device comprising:

a computer-readable medium or media encoded with instructions (claims 44-45) to

allow the computing device to perform the following tasks:

transmitting, from the computing device to the remotely located computing device, a

lock session signal for locking a secure communications session upon an occurrence of

a predetermined event, the lock session signal configured to restrict access to the

communications session until the computing device receives an unlock session signal

from the remotely located computing device (Fig. 8A, steps 510-550 wherein in step 510

a remote player inserts the player tracking card 312 into the card reader 310 (see Fig.

2); the player identity information is transmitted by the slot machine to the slot server 4,

which authenticates the information and creates a secure session with the player;

furthermore, in step 550, the remote player is prompted to enter the player parameter

selections; column 8, lines 10-33 disclose that the player parameter selections include

both play options and limiting criteria of play, wherein the limiting criteria include: (slot

machine) lock start time, lock end time, etc., the lock start time corresponding to a lock

session signal for locking a secure communications session upon an occurrence of a

predetermined event (lock start time), the lock session signal configured to restrict

access to the communications session until the computing device receives an unlock

session signal from the remotely located computing device; column 9, lines 1-6 disclose

the same details, further disclosing that the locking data is a signal that prevents the slot

machine 2 from providing access to other players unless automated play is terminated

by the player who initiated it);

prompting a user at the computing device for identification information associated with

the secure communications session (Fig. 9, steps 710-720 that show requiring the

player to return to the slot machine 2 and provide identification information associated

with the secure communications session; column 12, lines 14-17 describe the same

details);

transmitting, from the computing device to the remotely located computing device, the

identification information (Fig. 9, step 730 and column 12, lines 17-20 disclose the same

details); and

receiving, at the computing device from the remotely located computing device, the

unlock session signal if the identification information is authenticated (Fig. 9, steps 740

and 760-770; column 12, lines 21-39 describe the same details).

However, Walker et al. do not specifically disclose that **the predetermined event**

comprises a detection of a departure of the user without manual input from the

user.

In the same field of endeavor, Shaffer et al. disclose the claimed remotely

located computing device, **wherein the predetermined event comprises a detection**

of a departure of the user without manual input from the user (Fig. 2; column 5,

lines 13-32 which describe a security module 58 connected between the user

input device and the screen saver 56, that includes a timing mechanism that

monitors manipulation of the user input devices 44 to detect periods of inactivity;

further disclosing that the screen saver capability is configurable with respect to

selecting a particular time period, such that the screen saver 56 switches the

computing device 12 to a locked mode when the computing device is idle for a

period exceeding the pre-selected period; i.e. if there is no activity by any user

input devices for a configurable period, the screen saver triggers a locked mode

).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide means to detect the departure of a user as a predetermined event without any manual input from the user, as taught by Shaffer et al., in the computing device of Walker et al., so as to provide a secure remote session for users.

Consider **claim 70**, and **as it applies to claim 66 above**, Walker et al., as modified by Shaffer et al., further show and disclose the claimed computing device, including wherein the predetermined event further comprises a lapse in a predetermined amount of time (**in Walker et al. reference,** column 8, lines 22-33 which describe limiting criteria of play as any information that may define the beginning or end of an automated play session; further disclosing that lock start time is the elapse time, from the beginning of the session, used to lock the remote automated play session for a player who initiated the session, so that no other player may be allowed to use the same slot machine**; and in Shaffer et al. reference, Fig. 2; column 5, lines 13-32 that disclose the same details**).

Consider **claim 80**, and **as it applies to claim 66 above**, Walker et al., as modified by Shaffer et al., further disclose the claimed computing device, wherein the identification information is not a shared screen saver password (**in Walker et al. reference,** Figs. 2 and 9; column 12, lines 14-20 which disclose a player tracking card 312 that provides the player identification information for authentication by the slot

network server 4, thereby disclosing that the identification information is not a shared

screen saver password).

Consider **claim 82**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shaffer et al., further disclose the claimed computing device, wherein *the*

transmitting the lock session signal for the secure communications session *comprises*

transmitting the lock session signal to lock the communications session at the

remotely located computing device (**in Walker et al. reference,** Fig. 1 that shows a

slot machine 2 (a computing device) that communicates via slot network 3 with a slot

network server 4 (a remotely located computing device); column 3, line 60 through

column 4, line 18 describe the system shown in Fig. 1; Fig. 2 and column 4, lines 19-29

describe the details of the slot machine 2; Fig. 3 and column 5, lines 21-28 disclose the

details of the slot network server 4; column 8, lines 10-33 disclose that the player

parameter selections include both play options and limiting criteria of play, wherein the

limiting criteria include: (slot machine) lock start time, lock end time, etc., the lock start

time corresponding to a lock session signal for locking a secure communications

session upon an occurrence of a predetermined event (lock start time), the lock session

signal configured to restrict access to the communications session until the computing

device receives an unlock session signal from the remotely located computing device;

column 9, lines 1-6 disclose the same details, further disclosing that the locking data is

a signal that prevents the slot machine 2 from providing access to other players unless

automated play is terminated by the player who initiated it).

Consider **claim 84**, Walker et al. show and disclose a computer-readable

medium or media encoded with instructions for facilitating management of a secure

communications session (claims 44-45; Fig. 1 that shows a slot machine 2 (a computing

device) that communicates via slot network 3 with a slot network server 4 (a remotely

located computing device); column 3, line 60 through column 4, line 18 describe the

system shown in Fig. 1; Fig. 2 and column 4, lines 19-29 describe the details of the slot

machine 2; Fig. 3 and column 5, lines 21-28 disclose the details of the slot network

server 4), the instructions comprising code for:

transmitting, from the computing device to the remotely located computing device, a

lock session signal for locking a communications session upon an occurrence of a

predetermined event, the lock session signal configured to restrict access to the

communications session until the computing device receives an unlock session signal

from the remotely located computing device (Fig. 8A, steps 510-550 wherein in step 510

a remote player inserts the player tracking card 312 into the card reader 310 (see Fig.

2); the player identity information is transmitted by the slot machine to the slot server 4,

which authenticates the information and creates a secure session with the player;

furthermore, in step 550, the remote player is prompted to enter the player parameter

selections; column 8, lines 10-33 disclose that the player parameter selections include

both play options and limiting criteria of play, wherein the limiting criteria include: (slot

machine) lock start time, lock end time, etc., the lock start time corresponding to a lock

session signal for locking a secure communications session upon an occurrence of a

predetermined event (lock start time), the lock session signal configured to restrict

access to the communications session until the computing device receives an unlock

session signal from the remotely located computing device; column 9, lines 1-6 disclose

the same details, further disclosing that the locking data is a signal that prevents the slot

machine 2 from providing access to other players unless automated play is terminated

by the player who initiated it);

prompting a user at the computing device for identification information associated with

the communications session (Fig. 9, steps 710-720 that show requiring the player to

return to the slot machine 2 and provide identification information associated with the

secure communications session; column 12, lines 14-17 describe the same details);

transmitting, from the computing device to the remotely located computing device, the

identification information (Fig. 9, step 730 and column 12, lines 17-20 disclose the same

details); and

receiving, at the computing device from the remotely located computing device, the

unlock session signal if the identification information is authenticated (Fig. 9, steps 740

and 760-770; column 12, lines 21-39 describe the same details).

However, Walker et al. do not specifically disclose that *the predetermined event*

comprises a detection of a departure of the user without manual input from the

user.

In the same field of endeavor, Shaffer et al. disclose the claimed computer-

readable medium, *wherein the predetermined event comprises a detection of a*

departure of the user without manual input from the user (security system claim

11; Fig. 2; column 5, lines 13-32 which describe a security module 58 connected

between the user input device and the screen saver 56, that includes a timing

mechanism that monitors manipulation of the user input devices 44 to detect

periods of inactivity; further disclosing that the screen saver capability is

configurable with respect to selecting a particular time period, such that the

screen saver 56 switches the computing device 12 to a locked mode when the

computing device is idle for a period exceeding the pre-selected period; i.e. if

there is no activity by any user input devices for a configurable period, the screen

saver triggers a locked mode).

Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to provide a computer-readable medium with

executable instructions to detect the departure of a user as a predetermined event

without any manual input from the user, as taught by Shaffer et al., in the computer-

readable medium of Walker et al., so as to provide a secure remote session for users.

Consider **claim 85**, Walker et al. show and disclose a method for facilitating

management of a secure communications session from a remote computing device

(Fig. 1 that shows a method for facilitating management of a secure communications

session from a remote computing device, wherein a slot machine 2 (a computing

device) communicates via slot network 3 with a slot network server 4 (a remotely

located computing device); column 3, line 60 through column 4, line 18 describe the

method of communication shown in Fig. 1; Fig. 2 and column 4, lines 19-29 describe the

details of the slot machine 2; Fig. 3 and column 5, lines 21-28 disclose the details of the

slot network server 4), comprising the steps of:

transmitting, from the computing device to the remotely located computing device, a

lock session signal for locking a secure communications session upon an occurrence of

a predetermined event, the lock session signal configured to restrict access to the

communications session until the computing device receives an unlock session signal

from the remotely located computing device (Fig. 8A, steps 510-550 wherein in step 510

a remote player inserts the player tracking card 312 into the card reader 310 (see Fig.

2); the player identity information is transmitted by the slot machine to the slot server 4,

which authenticates the information and creates a secure session with the player;

furthermore, in step 550, the remote player is prompted to enter the player parameter

selections; column 8, lines 10-33 disclose that the player parameter selections include

both play options and limiting criteria of play, wherein the limiting criteria include: (slot

machine) lock start time, lock end time, etc., the lock start time corresponding to a lock

session signal for locking a secure communications session upon an occurrence of a

predetermined event (lock start time), the lock session signal configured to restrict

access to the communications session until the computing device receives an unlock

session signal from the remotely located computing device; column 9, lines 1-6 disclose

the same details, further disclosing that the locking data is a signal that prevents the slot

machine 2 from providing access to other players unless automated play is terminated

by the player who initiated it);

prompting a user at the computing device for identification information associated with

the communications session (Fig. 9, steps 710-720 that show requiring the player to

return to the slot machine 2 and provide identification information associated with the

secure communications session; column 12, lines 14-17 describe the same details);

transmitting, from the computing device to the remotely located computing device, the

identification information (Fig. 9, step 730 and column 12, lines 17-20 disclose the same

details); and

receiving, at the computing device from the remotely located computing device, the

unlock session signal if the identification information is authenticated (Fig. 9, steps 740

and 760-770; column 12, lines 21-39 describe the same details).

However, Walker et al. do not specifically disclose that *the predetermined event*

comprises a detection of a departure of the user without manual input from the

user.

In the same field of endeavor, Shaffer et al. disclose the claimed method,

wherein the predetermined event comprises a detection of a departure of the user

without manual input from the user **(Fig. 2; column 5, lines 13-32 which describe a**

security module 58 connected between the user input device and the screen

saver 56, that includes a timing mechanism that monitors manipulation of the

user input devices 44 to detect periods of inactivity; further disclosing that the

screen saver capability is configurable with respect to selecting a particular time

period, such that the screen saver 56 switches the computing device 12 to a

locked mode when the computing device is idle for a period exceeding the pre-

selected period; i.e. if there is no activity by any user input devices for a

configurable period, the screen saver triggers a locked mode).

Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to provide a method to detect the departure of a user

as a predetermined event without any manual input from the user, as taught by Shaffer

et al., in the method of Walker et al., so as to provide a secure remote session for users.

Claims 67, 68, 72-74, 77-79 and 81 are rejected under 35 U.S.C. 103(a) as

being unpatentable over **Walker et al. (U.S. Patent Publication # 6,244,957 B1)** in

view of **Shaffer et al. (U.S. Patent Publication # 6,145,083)** and further in view of

Shoemaker et al. (U.S. Patent Application Publication # 2005/0080915 A1).

Consider **claim 67**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shaffer et al., show and disclose the claimed computing device, except

wherein the computing device is configured to facilitate communication of the secure

communications session using a first communication channel and is configured to

facilitate communication of the lock session signal, the unlock session signal, and the

identification information using a second communication channel.

In the same field of endeavor, Shoemaker et al. disclose the claimed computing

device, wherein the computing device is configured to facilitate communication of the

secure communications session using a first communication channel and is configured

to facilitate communication of the lock session signal, the unlock session signal, and the

identification information using a second communication channel (Fig. 1B that shows

different channels being used for user interface (UI channel 210) and media (channel

208) transmission; paragraph 0087 discloses the same details).

Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to configure the computing device to facilitate

communication of the secure communications session using a first communication

channel and to facilitate communication of the lock session signal, the unlock session

signal, and the identification information using a second communication channel, as

taught by Shoemaker et al., in the computing device of Walker et al., as modified by

Shaffer et al., so that separate virtual channels may be provided for carrying serial

device communication and presentation data from the server, as well as encrypted

client mouse and keyboard data.

Consider **claim 68**, and **as it applies to claim 67 above**, Walker et al., as

modified by Shaffer et al. and Shoemaker et al., further show and disclose the claimed

computing device, wherein the second communication channel is a Citrix® Independent

Computing Architecture TM (ICA) Virtual Channel (in Shoemaker et al. reference,

paragraph 0086 which discloses that the second communication channel can be a

Citrix® Independent Computing Architecture TM (ICA) Virtual Channel).

Consider **claim 72**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shoemaker et al., further show and disclose the claimed computing device,

wherein the computing device is a personal computer (in Shoemaker et al. reference,

paragraphs 0054 and 0085 which disclose that the computing device can be a personal

computer).

Consider **claim 73**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shaffer et al. and Shoemaker et al., further show and disclose the claimed

computing device, wherein the computing device is an automated teller machine (ATM)

(in Shoemaker et al. reference, paragraph 0054 which discloses that the computing

device can be an Automated Teller Machine).

Consider **claim 74**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shaffer et al. and Shoemaker et al., further show and disclose the claimed

computing device, wherein the computing device is an industrial controller (in

Shoemaker et al. reference, paragraph 0054 which discloses that the computing device

can be an environment control element (industrial controller)).

Consider **claim 77**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shaffer et al. and Shoemaker et al., further show and disclose the claimed

computing device, wherein the computing device is a thin client (in Shoemaker et al.

reference, paragraphs 0003, 0082, 0084 and 0085 which disclose that the computing

device can be a thin client).

Consider **claim 78**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shaffer et al. and Shoemaker et al., further show and disclose the claimed

computing device, wherein the computing device is a personal digital assistant (PDA)

(in Shoemaker et al. reference, paragraph 0019 which disclose that the computing

device can be a personal digital assistant (PDA)).

Consider **claim 79**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shaffer et al. and Shoemaker et al., further show and disclose the claimed

computing device, wherein the computing device is a cellular telephone (in Shoemaker

et al. reference, paragraph 0019 which disclose that the computing device can be a

cellular telephone.

Consider **claim 81**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shaffer et al. and Shoemaker et al., further show and disclose the claimed

computing device, wherein the computing device is configured to allow a session

management operation to be triggered locally using an application at the computing

device, but executed at the remotely located computing device (in Shoemaker et al.

reference, paragraph 0088 which disclose that a virtual channel application has two

parts, a client-side component and a server-side component; further disclosing that the

server-side component is an executable program running on the terminal server, and

the client-side component is a DLL loaded into memory on the client computer when the

terminal services client program runs).

Claims 71 and 76 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Walker et al. (U.S. Patent Publication # 6,244,957 B1) in view of Shaffer et al.

(U.S. Patent Publication # 6,145,083) and further in view of Hughes (U.S. Patent

Publication # 6,854,009 B1).

Consider claim 71, and as it applies to claim 66 above, Walker et al., as

modified by Shaffer et al., show and disclose the claimed computing device, except

wherein the predetermined event is an activation of a screen saver.

In the same field of endeavor, Hughes discloses the claimed computing device,

wherein the predetermined event is an activation of a screen saver (column 27, lines

37-53 disclose the same details).

Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to activate a screen saver at the predetermined event,

as taught by Hughes, in the computing device of Walker et al., as modified by Shaffer et

al., so as to maintain the security during the period, the user of the computing device is

away from the remote session.

Consider claim 76, and as it applies to claim 66 above, Walker et al., as

modified by Shaffer et al. and Hughes, further show and disclose the claimed computing

device, wherein the computing device is an internet protocol (IP) telephone (in Hughes

reference, Fig. 5, column 6, lines 55-62 and column 11, lines 30-39 that disclose the

details of the claimed IP telephone).

Claim 75 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Walker**

et al. (U.S. Patent Publication # 6,244,957 B1) in view of **Shaffer et al. (U.S. Patent**

Publication # 6,145,083) and further in view of **Hsu et al. (U.S. Patent Publication #**

6,876,644 B1).

Consider **claim 75**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shaffer et al., show and disclose the claimed computing device, except

wherein the computing device is a gateway.

In the same field of endeavor, Hsu et al. disclose the claimed computing device,

wherein the computing device is a gateway (column 6, line 56 through column 7, line 9

which disclose that the proxy gateway server 20 selectively controls access by the

digital telephone 16 to additional servers via a packet switched network and based on

the validation of security information supplied by the digital telephone).

Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to use a gateway as a computing device, as taught by

Hsu et al., in the computing device of Walker et al., as modified by Shaffer et al., so as

to provide a secure remote session.

Claims 83 and 86 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Walker et al. (U.S. Patent Publication # 6,244,957 B1) in view of Shaffer et al.

(U.S. Patent Publication # 6,145,083) and further in view of Wright et al. (U.S. Patent

Publication # 7,089,508 B1).

Consider claim 83, and as it applies to claim 66 above, Walker et al., as

modified by Shaffer et al., further disclose the claimed computing device, wherein the

computing device is configured to facilitate a session lock at the remotely located

computing device (in Walker et al. reference, Fig. 8A, steps 510-550 wherein in step

510 a remote player inserts the player tracking card 312 into the card reader 310 (see

Fig. 2); the player identity information is transmitted by the slot machine to the slot

server 4, which authenticates the information and creates a secure session with the

player; furthermore, in step 550, the remote player is prompted to enter the player

parameter selections; column 8, lines 10-33 disclose that the player parameter

selections include both play options and limiting criteria of play, wherein the limiting

criteria include: (slot machine) lock start time, lock end time, etc., the lock start time

corresponding to a lock session signal for locking a secure communications session

upon an occurrence of a predetermined event (lock start time), the lock session signal

configured to restrict access to the communications session until the computing device

receives an unlock session signal from the remotely located computing device; column

9, lines 1-6 disclose the same details, further disclosing that the locking data is a signal

that prevents the slot machine 2 from providing access to other players unless automated play is terminated by the player who initiated it).

However, Walker et al., as modified by Shaffer et al., do not specifically disclose that the computing device is configured to facilitate a local lock at the computing device.

In the same field of endeavor, Wright disclose the claimed computing device, wherein the computing device is configured to facilitate a local lock at the computing device (abstract that discloses a method for preventing the activation of a screen saver for locking user access to a computer while a user is near the computer; column 1, lines 12-38 disclose an office personal computer, for use by a plurality of users, that uses the screen saver lock access to the computer after a specified period of keyboard or mouse inactivity; further disclosing that authorized users may gain access to the locked local computer by entering their userid and the common password).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to configure the computing device to facilitate a local lock at the computing device, as taught by Wright, in the computing device of Walker et al., as modified by Shaffer et al., so as to provide a secure computing environment for a local shared computing device.

Consider **claim 86**, and **as it applies to claim 66 above**, Walker et al., as modified by Shaffer et al. and Wright et al., further disclose the claimed computing device, wherein the detection of the departure of the user without manual input from the user is performed using at least one of the following without manual input by the user

indicating the departure: a motion detector, a presence or an absence of a dedicated

short range communication identification device, or an altered biometric data of the user

(in Shaffer et al. reference, column 1, lines 42-46 which disclose using biometric

technique such as voiceprint authentication to recognize an authorized user; and

in Wright et al. reference, column 1, lines 56-58 which describe a controller that includes

a motion sensor, such as a motion detector, for detecting o user's activity (and

presence) within a predetermined perimeter of the computer whose screen may be

locked; also see Figs. 11, 18 and column 5, lines 26-49 in the cited but not used

reference (US Patent Publication 7,069,444 B2 to Lowensohn et al.) that uses biometric

data for detecting user's presence).

Claim 87 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Walker

et al. (U.S. Patent Publication # 6,244,957 B1)** in view of **Shaffer et al. (U.S. Patent

Publication # 6,145,083)** and further in view of **Hendriks et al. (U.S. Patent

Publication # 7,219,233 B1).**

Consider **claim 87**, and **as it applies to claim 66 above**, Walker et al., as

modified by Shaffer et al., disclose the claimed computing device, except wherein the

detection of the departure of the user without manual input from the user is performed

by software configured to use artificial intelligence to examine input or writing style of

another user.

In the same field of endeavor, Hendriks et al. show and disclose the claimed

computing device, wherein the detection of the departure of the user without manual

input from the user is performed by software configured to use artificial intelligence to

examine input or writing style of another user (Fig. 6; column 9, lines 27-30 that teach

using artificial intelligence in identifying a user by analyzing the physical dynamics of the

user's handwriting as is done in signature verification and/or handwriting analysis).

Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to use software configured to use artificial intelligence

to examine input or writing style of a user, as taught by Hendriks et al., in the computing

device of Walker et al., as modified by Shaffer et al., so as to provide a secure

computing environment for an unattended computing device.

Response to Arguments

Applicant's arguments with respect to claims 66-68 and 70-85 have been

considered but are moot in view of the new ground(s) of rejection.

Conclusion

The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure:

US Patent: 7,069,444 B2, inventor: Lowensohn et al., issued: 06/27/2006

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed**

to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Art Unit: 2443

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the

Examiner should be directed to Kishin G. Belani whose telephone number is (571) 270-

1768. The Examiner can normally be reached on Monday-Friday from 6:00 am to 5:00

pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's

supervisor, Tonia Dollinger can be reached on (571) 272-4170. The fax phone number

for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist/customer service whose telephone

number is (571) 272-2600.

/K. G. B./
Examiner, Art Unit 2443

September 29, 2009

/George C Neurauter, Jr./

Primary Examiner, Art Unit 2443